Quantum Computing and Cryptography

Table of contents

1. Quantum computing threat to current cryptography

1.1. Why is the quantum computer such a disruption to our technology?

The information unit of classical computing is called "bit" (binary digit) and has two basis states namely 0 and 1. Modern computers use combinations of these two basis states for encoding all information discernible to humans in a deterministic manner.

Drawing parallels to classical computing, quantum computing uses an information unit called "qubit" (quantum bit) which has two basis quantum states (Box 1.1).

> A quantum state is a mathematical entity that provides a hidden probability distribution for the outcomes of each possible measurement on a quantum system. Knowledge of the quantum state together with the rules of quantum mechanics aids in understanding the quantum system's behaviour.

Box 1.1: Quantum state

A qubit is a two-level quantum system where the two basis quantum states are usually expressed using bra-ket notation (Box 1.2).

> The bra-ket notation (aka Dirac notation) is used to denote quantum states. The notation uses the angle brackets ⟨ and ⟩ and the vertical bar | to construct "bras" and "kets". Bra–ket notation was created by English theoretical physicist Paul Adrien Maurice Dirac.

Box 1.2: Bra-ket notation

The qubit's basis quantum states are written as $|0\rangle$ and $|1\rangle$. A qubit can be in state $|0\rangle$, in state $|1\rangle$ or, unlike a classical bit, in a linear combination $\alpha|0\rangle + \beta|1\rangle$ of both states (where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$ according to the Born rule, see Box 1.3). The name of this phenomenon is superposition.

> In a superposition of quantum states, the squared norm of the amplitude of a state is the probability of that state resulting after measurement, Furthermore, the sum of the squared norms of the amplitudes of all possible states in the superposition is equal to 1.
>
> The amplitudes α and β are complex numbers.
>
> The vertical bars | and | denote the norm (aka modulus) $|z|$ of a complex number $z = a + bi$, which is the length of the vector from the origin to the point (a, b) in a two-dimensional plane. According to the Pythagorean theorem $|z|$ is the square root of $a^2 + b^2$.

Box 1.3: Born rule

As the information units in classical and quantum computing have fundamental different properties, quantum computations also follow a fundamentally different approach compared to classical computations. Firstly, the input to a quantum computation can be transformed by means quantum superposition. This enables a quantum computation to take into account multiple

quantum state combinations simultaneously, resulting in quantum parallelism. Secondly, a quantum computation can make use of quantum entanglement.

> Quantum entanglement is a physical phenomenon that occurs when a group of particles are generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the group cannot be described independently of the quantum state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical physics and quantum mechanics.

Box 1.4: Quantum entanglement

A quantum computation is performed by applying a series of quantum gates (i.e. a quantum circuit) to the qubits (Box 1.5).

> A quantum gate is an operation applied to one or more qubits. A quantum circuit is a computational routine consisting of coherent quantum operations on qubits. It is an ordered sequence of operations by quantum gates on a set of qubits.

Box 1.5: Quantum gate / quantum circuit

At the end of a quantum computation, the qubits are measured. In contrast to the result of a classical computation, the result of the measurement of the qubits (Box 1.6) is in general probabilistic. The measurement must therefore be repeated multiple times in order to obtain the desired output (i.e. the result which has the highest probability of occurrence), by averaging the results of a series of repeated measurements.

> A quantum measurement is the testing or manipulation of a quantum system to yield a numerical result. The predictions that quantum mechanics makes about these measurements are in general probabilistic and depend on the state of the quantum system that is being measured. The main objective of quantum computing is to execute a quantum circuit to set up the system's quantum state in such a way that (the) desired measurement outcome(s) have a high probability of occurring.

Box 1.6: Quantum measurement

The main objective of quantum computing is to execute a quantum circuit to transform the system's quantum state in such a way that the desired outcome has a high probability of occurring.

Taking the above into account, one can already imagine that quantum computing will offer new means to solve otherwise intractable computational problems. Furthermore, quantum parallelism makes it easy to scale up, because adding just one qubit in principle doubles the computing capacity of a quantum computer.

Some known 'hard problems' can be solved exponentially faster with a quantum computer. This opens new avenues with immense potential, for example for developing new chemical processes, new drugs, and new communication, security and cryptographic protocols. At the same time, it

may impact the security offered by currently deemed unbreakable public-key cryptographic algorithms, which would have major consequences for data confidentiality protection.

It should however be noted that quantum computing will not outperform modern classical computing in all aspects.

Furthermore, due to a lack of stable physical qubits, the capabilities of contemporary quantum computers are seveerly limited because random noise may corrupt the desired output of quantum computations.

Several companies have created quantum computers based on different qubit technologies. These qubits are constructed from different materials and most of them operate in strictly controlled environments as there are a lot of factors that can influence the reliability of the state of a qubit like heat, magnetism, light, etc. Error correction is needed to increase the actual reliability of such qubits. One way of performing error correction is to deploy multiple imperfect 'physical qubits' which jointly form the representation of a 'logical qubit' (aka noiseless qubit or error-proof qubit).

1.2. Threats by Quantum Computers

The most common and well-known encryption method is symmetric encryption aka secret-key encryption. Symmetric encryption algorithms use the same secret key for both encryption of the plaintext and decryption of the encrypted text (aka ciphertext). The secret key is shared by the communicating parties.

Advanced Encryption Standard (AES) is an example of a symmetric encryption algorithm.

A major advantage of symmetric encryption is its speed, a major disadvantage is that the shared secret key is known to the communicating parties. And if you have multiple communication partners, you will need a unique key for every communication partner, quickly resulting in an untenable situation in terms of scaling up. Therefore, symmetric encryption algorithms always lead to key distribution concerns.

Asymmetric encryption aka public-key encryption algorithms distinguish themselves by the fact that they use two different keys that together form a single key pair. What is encrypted with one key can be decrypted only by using the other associated key. This makes it possible to make one key (the public key) publicly known, after which anyone can use this public key to encrypt a message for the owner of the other key (the private key). Needless to say that the private key must be protected to make sure that only the owner is able to decrypt the message.

RSA (Rivest, Shamir and Adleman), DH (Diffie-Hellman) and ECC (Elliptic Curve Cryptography) are examples of public-key cryptographic algorithms.

Based on the feature that what is encrypted with a public key can be decrypted only by using the associated private key, a sender can encrypt a message using the receiver's public key and that

encrypted message can be decrypted only by using the receiver's private key. This is a major advantage because it removes the need of a secure channel for the initial exchange of one or more secret keys between the communicating entities. The drawback is that public-key cryptography is computationally intensive, compared with symmetric encryption.

Practically all today's security protocols (Box 1.7) use a combination of symmetric and asymmetric cryptography. Typically, bulk data that is exchanged during a communication session is secured with symmetric encryption for performance reasons. However, due to the advantages that asymmetric cryptography offers, it is also commonly used, for example for authentication of the communicating entities at the start of a session and for the exchange of the symmetric encryption session key that is used to secure the bulk data.

A security protocol like Transport Layer Security (TLS) describes how the encryption algorithms like AES and RSA should be used. A detailed security protocol includes details about data structures, representations and whether it can be used with interoperable versions.

Box 1.7: Example of security protocol

In general, we can state that cryptographic algorithms raise a computational barrier. However, the hard problems of classical cryptography are tailored to the currently available classical computation power. But some of the hard problems of today turn out to be easy solvable with a quantum computer. We already know two quantum algorithms that have a high impact on our current classical cryptography:

1. Shor's algorithm, named after the mathematician Peter Williston Shor, is an algorithm formulated in 1994 that provides exponential speedup over classical counterparts for integer factorisation and related public-key encryption primitives. This implies that almost all public-key encryption algorithms are in danger of being broken using Shor's algorithm, unless extremely large (and therefore impractical) key sizes are used.

2. Grover's algorithm, named after the computer scientist Lov Kumar Grover is a search algorithm formulated in 1996 that finds, with high probability, the unique input to a black box function that produces a particular output value. Grover's algorithm provides a quadratic speedup (x versus x^2) over a classical computer search algorithm, which means it can solve a problem on a quantum computer with 1,000 steps that would take 1,000,000 steps on a classical computer. Although not as impressive as exponential speedup, the quadratic speedup is considerable and affects the security levels provided by both symmetric encryption algorithms and hash algorithms.

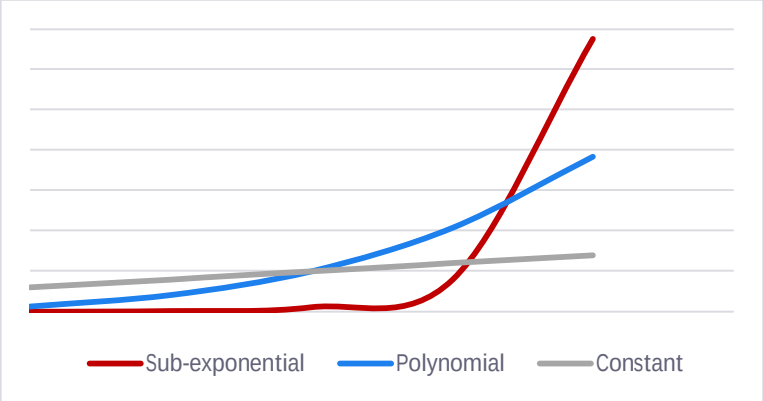
The sizes of cryptographic keys that are commonly used for RSA, DH and ECC cryptography depend on both the desired level of bit security (n-bit security) and the efficiency of the best-known classical attack against the underlying hard problem.

For the Integer Factorization Problem (IFP) underlying RSA cryptography, the best-known problem solving algorithm, i.e. the General Number Field Sieve (GNFS), has a sub-exponential

complexity. For the Discrete Logarithm Problem (DLP) problem underlying DH cryptography (which is almost exclusively used for secret key exchange purposes), the best-known problem solving algorithm, i.e. the Index-Calculate Method (ICM), also has a sub-exponential complexity. In contrast, for the Elliptic Curve Discrete Logarithm Problem (ECDLP) problem underlying ECC cryptography, the best-known solving algorithm, i.e. Pollard's Rho, has an exponential complexity. In fact, the lack of known solving algorithms of sub-exponential complexity has made ECC cryptography more attractive than RSA cryptography, because it means that its cryptographic keys can have much smaller sizes than those of RSA for the same level of n-bit security.

In computational complexity theory, polynomial time refers to the computation time of a problem where the run time, m(n), is no greater than a polynomial function of the problem size, n. Written mathematically using 'big O' notation, this states that $\mathbf{m(n) = O(n^k)}$ where **k** is some constant that may depend on the problem. For example, the classical 'quicksort' sorting algorithm on **n** integers performs at most $\mathbf{An^2}$ operations for some constant **A**. Thus it runs in $\mathbf{O(n^2)}$ time and is a polynomial time algorithm.

Sub-exponential time refers to the computation time of a problem where the run time is greater than a polynomial function but smaller than an exponential function of the problem size. For example, the best-known classical algorithm for integer factorisation, the General Number Field Sieve (GNFS), runs in about $\mathbf{O\left(2^{\log n}\right)^{\frac{1}{3}}}$ time for the factoring of an integer **n**.



Example graph

Box 1.8: Explanation of polynomial time and sub-exponential time

The advent of powerful quantum computers will change the rules of the game. Shor's quantum algorithm will be capable of solving the IFP, DLP and ECDLP problems in polynomial time, once a sufficiently large Fault-Tolerant Quantum Computer (FTQC) is available. This algorithm is actually composed of three parts: a Quantum Fast Fourier Transform (QFFT) part, which is a purely quantum part, a purely classical pre-processing part and a purely classical post-processing part. From a computing complexity standpoint, the QFFT part has polynomial time complexity.

For factoring n-bit integers, a FTQC quantum computer running Shor's algorithm will need at least n logical qubits to represent the integer and will also require additional working logical quantum bits. Various quantum circuit versions capable of running QFFT have been proposed for reducing the number of logical qubits required. The current state-of-the-art of these quantum circuits requires a number of logical qubits that is roughly three times the bit size of the integer to be factored.

The situation is different in the case of elliptic curves. Shor's algorithm can be used to efficiently solve the ECDLP problem in polynomial time, but because of how the classical parts of the algorithm need to embed elliptic curve points representation into a larger group, the number of logical qubits required is roughly ten times the bit size of the elliptic curve field.

One might be tempted to say that the above implies that ECC cryptography is more resilient to quantum computing attacks than RSA cryptography, because mounting an attack on ECC at first sight appears to require more logical qubits than an attack on RSA does. But it is exactly the opposite, the reason being that RSA cryptography needs to use very large keys in order to resist classical attacks hence the required logical qubit count for the same level of n-bit security is actually larger for RSA than for ECC. It just turns out that the existence of classical attacks of sub-exponential complexity on RSA, compared to the existing classical attacks of exponential complexity on ECC, has made its current use more resilient to quantum attacks!

1.3. Impact according worst case scenarios

According to a worst-case scenario we can make current classical symmetric encryption algorithms Grover resilient by doubling the key length. For an algorithm like AES this is not a problem but for DES this is however not possible. Concerning cryptographic hash functions, the Grover algorithm seems to provide some non-trivial quadratic speedup. Nevertheless, when doubling the output of the hash function we should be fine. For a cryptographic hash algorithm like SHA-2 this is not a problem but for MD5 this is however not possible.

Shor's algorithm will have the biggest impact, because most commonly used public-key cryptographic algorithms can be considered broken.

If we take into account the resources needed to implement the Grover or Shor algorithms to break current cryptographic schemes, these resources are not yet available. To this date, quantum computing does not yet constitute a real threat. At the moment this will happen, referred to as *day z*, there will be varying degrees of impact on some notable and popular kinds of cryptography. The difficulty of putting a date to this moment does not reduce the impact of the inevitable consequences, but it may delay the prioritisation of mitigation.

So how to continue? Mosca's theorem (Figure 1.9) could be helpful here. In brief: If $x + y > z$ then we have a problem with a particular cryptographic scheme (a cryptographic algorithm using a particular key size):

x is the security shelf life; it refers to how long data encrypted with this particular cryptographic scheme must remain secure against quantum attacks after post-quantum migration has been completed;

y is the migration time; it refers to how much time we need to migrate from this particular cryptographic scheme to a quantum-secure cryptographic scheme;

z refers to the time when a quantum computer will be available that breaks this particular cryptographic scheme.

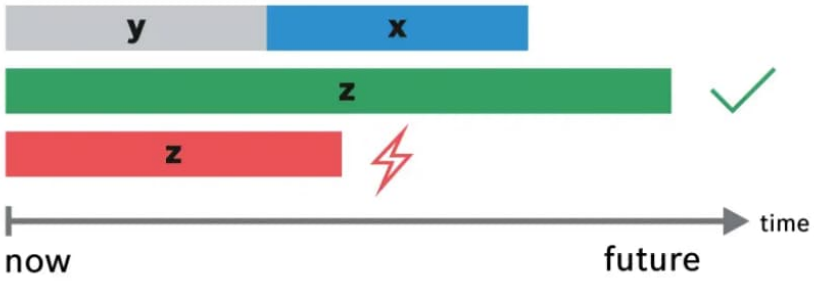


Figure 1.9: Mosca's theorem

In other words: there is a problem if the time to migrate to a quantum-secure cryptographic scheme plus the security shelf life is beyond the time when a quantum computer will be capable of breaking the particular cryptographic scheme. Therefore, if you have to ensure the confidentiality of some data for a very long period of time, you may have a significant challenge at hand.

Furthermore, if the encrypted data is exchanged over a public communications channel, an adversary may intercept the communication, store the encrypted communication and wait for the moment when the cryptographic scheme that has been used can be broken to retroactively decrypt the data that was exchanged (a so-called 'store now, decrypt later' attack). This is a challenge that some organisations, including our governments, are already facing right now.

The key question is: Which type of encryption is still secure in the era of the quantum computer? For symmetric encryption algorithms and hash algorithms, we have already seen that the quantum computing threat can be mitigated by doubling the key or hash value size. For public-key encryption algorithms we however do need alternatives.

1.4. Quantum threat taxonomy

A structured list of examples of various types of cyberattacks enabled by the malicious use of quantum computing is provided below. These attacks could be performed in the future when powerful quantum computers will be available, if at that time cryptographic schemes are still being used that are not quantum-resistant. Some attacks, the so-called "harvest now, decrypt later" attacks, could already be attempted today if non-quantum-resistant cryptography is being used.

- Harvesting of encrypted data for malicious purposes:
    - harvesting of encrypted data-in-transit:
        - mass data harvesting;
        - event-based data harvesting;
        - target-based data harvesting (targeting specific organisations or individuals);
        - etc.
    - harvesting of encrypted data-at-rest:
        - application data files and databases;
        - snapshots and backups;
        - archival data;
        - etc.
    - harvesting of encrypted data-in-use:
        - application-level data encryption;
        - Virtual Machine Image (VMI) encryption;
        - etc.
- Malicious signing of digital artefacts[1]:
    - malicious code signing:
        - fake firmware/software and updates;
        - fake malware fingerprints;
        - etc.
    - fraudulent manipulation of digital legal documents:
        - fake passports, birth certificates, driving licences, etc.;

[1] The word "fake" refers to "malicious modification or malicious fabrication".

        - fake ownership records;
        - fake mortgage and loan contracts;
        - fake intellectual property (patents and trademarks);
        - etc.
    - fraudulent manipulation of digital evidence:
        - fake audit records (financial, legal, etc.);
        - fake forensic records;
        - fake criminal records;
        - etc.
    - malicious signing of other digital artefacts:
        - fake diplomas and licences;
        - fake insurance policies and claims;
        - fake invoices;
        - fake tax records;
        - fake compliance certificates (quality, security, etc.);
        - etc.
- Malicious data origin authentication: modification or fabrication of integrity proofs associated with digital artefacts.
- Malicious entity authentication:
    - issuing of fake credentials;
    - impersonation;
    - privilege escalation;
    - etc.

Many of these attacks can be performed offline and may take several hours or (much) more to complete using a shared-access quantum computing service. However, some attacks must be

performed online in just a few seconds, thus requiring real-time dedicated access to powerful quantum computers.

2. Status of potential future solutions

2.1. Introduction

Cryptography is often the strongest link in the chain of data security. However, it cannot be assumed that cryptographically protected data will remain secure indefinitely. When using classical cryptography, security of encrypted data can typically not be guaranteed beyond approximately 30 years[2]. Some use-cases, for example confidentiality protection of patients' medical records, may require longer periods of protection. Quantum cryptography (§ 2.3) has the potential to provide protection for such long periods.

The security of (classical) public-key cryptographic algorithms, which are widely used today, relies on one of three hard mathematical problems (IFP, DLP and ECDLP), which are computationally too difficult to solve with current and projected future classical computers, but could be solved by future Cryptographically Relevant Quantum Computers[3] (CRQCs) executing (a variant of) Shor's quantum algorithm.

There are two main directions for developing solutions to counter the threats posed by CRQC's to classical public-key cryptographic algorithms:

1. **Quantum-Resistant Cryptography (QRC)**, which runs on classical (non-quantum) computing platforms (§ 2.2);

2. **Quantum cryptography** (a misnomer for "**secure quantum communication**"), which is a form of "cryptography" that exploits quantum mechanics phenomena (§ 2.3).

2.2. Quantum-Resistant Cryptography (QRC)

Quantum-Resistant Cryptography (QRC) is also referred to as quantum-proof cryptography, quantum-safe cryptography or quantum-secure cryptography. It should however be noted that such cryptographic schemes are not really quantum-proof, quantum-safe or quantum-secure, but merely quantum-resistant, since it is not known or provable that there will not be potential future successful classical or quantum attacks against them.

---

[2] The One-Time Pad (OTP) is the only encryption scheme that –theoretically- cannot be broken, but it requires the use of single-use pre-shared keys that are not smaller than the messages being encrypted/decrypted. OTP is therefore impractical for most applications.

[3] The term Cryptographically Relevant Quantum Computer (CRQC) is used to specifically describe powerful future quantum computers that are capable of actually attacking real world cryptographic schemes that would be infeasible to attack with a classical computer.

On 11 August 2015, the US National Security Agency (NSA) took everybody by surprise by announcing their plan to transition to quantum-resistant cryptographic algorithms. It moved away from the Suite B cryptographic algorithms specified by the US National Institute of Standards and Technology (NIST) by explaining that "*unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many hoped it would be. Thus, we have been obligated to update our strategy.*"

In April 2016, NIST started a Post-Quantum Cryptography (PQC) competition with the aim to identify and standardise new quantum-resistant public-key encryption algorithms, to replace the ones that are vulnerable to attacks by means of future CRQCs.

In July 2022, NIST announced four candidate algorithms for standardisation: CRYSTALS-Kyber (key establishment scheme), CRYSTALS-Dilithium (digital signature scheme), FALCON (digital signature scheme) and SPHINCS+ (digital signature scheme). In August 2023, NIST released draft FIPS standards for these PQC algorithms. NIST also announced three candidate key establishment schemes that will advance to the fourth round of the PQC competition: BIKE, Classic McEliece and HQC. In August 2024, NIST released FIPS standards for three PQC algorithms:

1. FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), based upon the CRYSTALS-Kyber algorithm;

2. FIPS 204 - Module-Lattice-Based Digital Signature Algorithm (ML-DSA), based upon the CRYSTALS-Dilithium algorithm;

3. FIPS 205 - Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), based upon the SPHINCS+ algorithm.

The fourth standard, FIPS 206 - FFT over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA) , based on FALCON is expected to be released in 2024.

After standardisation of the first set of PQC algorithms, NIST's PQC effort will continue for many years to come. This effort will not only consist of updating and refining the published PQC standards, but also intends to identify potential new PQC algorithms and to ensure that there are strong back-ups for selected PQC standards, as the full extent of what might emerge in the area of CRQCs and their associated quantum algorithms remains unknown.

To diversify its signature scheme portfolio, NIST issued a call for proposals for additional quantum-resistant signature schemes in September 2022. In July 2023 NIST had received 50 submissions, of which 40 satisfy all submission requirements. NIST then initiated a new process for thorough evaluation of these signature schemes, which is expected to take several years to complete. Based on the public feedback and internal reviews of the first-round candidates, NIST announced the selection of 14 digital signature algorithms as second-round candidates in

October 2024 to move forward to the next stage of the standardisation process. These candiates are:

- MPC-in-the-Head schemes: MIRA, MiRitH, MQOM, PERK, RYDE and SDithH;
- code-based schemes: CROSS and LESS;
- structured lattice-based scheme: HAWK;
- multivariate-based schemes: MAYO, QR-UOV, SNOVA and UOV;
- isogeny-based scheme: SQIsign;
- symmetric-based scheme: FAEST.

It is important to recognise that most of the currently proposed PQC schemes have not received nearly as much scrutiny from the cryptographic community as the currently widely used public-key cryptographic schemes. Further analysis and research may uncover that these PQC schemes are not secure enough for replacement of the currently deployed public-key cryptographic schemes.

It should also be noted that QRC involves more than NIST's PQC schemes. For example, there were already some special public-key cryptographic algorithms (such as XMSS), which turned out to be quantum-resistant when Shor published his famous quantum algorithm in 1994. Due to their particular characteristics, these algorithms are however limited to specific use cases.

It is expected that standardisation organisations, such as for example the IETF, will start working on modifications and extensions of existing security protocol standards, such as for example TLS, that are required in order to support the new PQC cryptographic schemes.

Several open-source projects and libraries already implemented QRC cryptographic schemes. For example, OpenSSL and OpenSSH provide support for several PQC algorithms through integration with liboqs, an open-source C library for QRC algorithms that is part of the Open Quantum Safe (OQS) project[4]. The following QRC algorithms are currently supported by liboqs:

- KEM schemes: BIKE, Classic McEliece, CRYSTALS-Kyber, FrodoKEM, HQC and NTRU-Prime;
- digital signature schemes: Dilithium, FALCON and SPHINCS+.

QRC schemes are also already implemented in commercially available products; for example:

- Amazon implemented the BIKE, CRYSTALS-Kyber and SIKE KEM schemes into TLS used by its AWS Key Management Service, AWS Certificate Manager and AWS Secrets Manager;
- CloudFlare implemented CRYSTALS-Kyber into TLS used in its CDN infrastructure and also implemented several QRC algorithms in its CIRCL library;

[4] In February 2024, The OQS project was transferred to the Post-Quantum Cryptography Alliance (PQCA). PQCA aims to be the central foundation for organisations and open source projects seeking production-ready libraries and packages, to support their alignment with the US NSA's Cybersecurity Advisory concerning the Commercial National Security Algorithm Suite 2.0.

- Entrust implemented CRYSTALS-Dilithium and FALCON into its nShield HSMs[5];
- Google implemented CRYSTALS-Kyber in the Chrome browser and also implemented CRYSTALS-Dilithium combined with ECDSA in its FIDO2 security keys;
- IBM implemented CRYSTALS-Kyber, CRYSTALS-Dilithium and FALCON in several products, including IBM Hyper Protect Crypto Services, IBM z16 mainframes, IBM tape storage, IBM Power, Red Hat and IBM HSMs;
- Utimaco implemented CRYSTALS-Kyber, CRYSTALS-Dilithium, HSS, LMS, XMSS and XMSSMT into its HSMs.

Specialised cryptographic security vendors provide QRC implementations as hardware or software building blocks for integration into products marketed by other vendors or service providers. For example, Infineon implemented XMSS in its OPTIGA TPM and NXP implemented CRYSTALS-Dilithium in its S32G Vehicle Network Processors.

A common characteristic of several QRC schemes is that they require larger cryptographic key sizes or produce digital signatures or ciphertexts with larger size than the commonly used pre-quantum public-key cryptographic algorithms. Other QRC schemes have large storage requirements and/or consume a large amount of computing cycles. In some cases, QRC scheme characteristics can be adjusted by appropriate setting of the scheme's parameters; this often involves a delicate trade-off between performance and security.

Resistance to Side-Channel Attacks (SCAs) and misuse-resistance are also considered important QRC scheme characteristics (some QRC schemes provide better SCA resistance and/or misuse-resistance than others). Simplicity and flexibility (e.g. suitability for implementation on ICT platforms with limited computing and/or memory resources) are other important distinguishing characteristics of QRC schemes.

2.3. Quantum cryptography

Quantum cryptography exploits quantum mechanics properties to perform cryptographic tasks. Currently, the best-known examples of quantum cryptography are Quantum Random Number Generator (QRNG) and Quantum Key Distribution (QKD).

QRNG and QKD -in theory- provide information-theoretically secure solutions that are not possible using only classical (non-quantum) mechanisms. It should be noted that the information-theoretic security of QRNG and QKD as claimed by the vendors (and occasionally also by the

[5] A Hardware Security Module (HSM) is a cryptographic module in the form of a USB-stick, a plug-in card or an external device attached directly to a computer or via a network connection. A HSM safeguards and manages cryptographic keys (including random key generation), performs encryption/decryption functions, performs cryptographic functions for generation/verification of digital signatures, strong authentication, etc.

media) is based on the laws of quantum mechanics. However, the security of quantum encryption technology is highly implementation-dependent rather than assured by quantum mechanics laws.

The UK National Cyber Security Centre (NCSC) does not endorse the use of QRNG and QKD for government or military applications and advises to continue using classical RNGs and to use NIST PQC instead of QKD solutions. In particular, the NCSC believes that classical RNGs will continue to meet the needs of government and military applications for the foreseeable future. Similar advice is given by the French ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), the German BSI (Bundesamt für Sicherheit in der Informationstechnik) and the Dutch NCSC (Nationaal Cyber Security Centrum) and AIVD/NBV (Algemene Inlichtingen- en Veiligheidsdienst / Nationaal Bureau voor Verbindingsbeveiliging).

2.3.1. Quantum Random Number Generator (QRNG)

Quantum Random Number Generators (QRNGs) exploit the inherent randomness of quantum mechanics to generate truly random numbers. Various products based on QRNG are currently being developed or already commercially available from a number of vendors in various form factors; for example:

- QRNG chip, e.g. for use in small Internet-of-Things (IoT) devices;
- Q-PUF chip, which is a combination of a QRNG and a Physically Unclonable Function (PUF)[6];
- QRNG USB-stick;
- QRNG PCIe card[7];
- mobile phone with embedded QRNG chip;
- Quantum Hardware Security Module (QHSM), which implements QRNG to generate random encryption keys;
- Quantum Entropy-as-a-Service (Q-EaaS)[8];
- QRNG quantum algorithm.

QRNG is typically implemented with QRNG building blocks provided by OEM manufacturers of quantum security technology.

---

[6] A Physically Unclonable Function (PUF) is a physical entity that is embodied in a physical structure and is easy to evaluate but hard to predict. All PUFs are subject to environmental variations such as temperature, supply voltage and electromagnetic interference, which can affect their performance. Therefore, rather than just being random, the real power of a PUF is its ability to be different between devices, but simultaneously to be the same for a specific device under varying environmental conditions.

[7] Peripheral Component Interconnect Express (PCIe) is a high-speed serial computer expansion bus standard. It is the common motherboard interface for personal computers' graphics cards, sound cards, hard disk drive host adapters, SSDs, Wi-Fi and Ethernet hardware connections.ZA

[8] Entropy is a scientific concept as well as a measurable physical property that is most commonly associated with a state of disorder, randomness or uncertainty.

The QRNG QSG Workgroup hosted by the EITCI Institute, in cooperation with CEN/CENELEC, ETSI, ITU-T, IETF, ANSI/ASC, NIST and ISO/IEC is developing technical reference standards for both Entanglement-based QRNG (EQRNG) and Non Entanglement-based QRNG (NEQRNG).

Main QRNG limitations are:

- use of QRNG products in Virtual Machine (VM) and containerised environments is problematic;
- limited QRNG standardisation;
- validating QRNG implementations is a significant challenge.

2.3.2. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is used to produce and distribute shared secret encryption keys, not to encrypt/decrypt transmitted data. QKD security is based on the no-cloning theorem of quantum mechanics which makes it impossible to copy data encoded in a quantum state (Box 2.1): if reading of quantum-encoded data is attempted, its wave function collapses. This results in a change of its quantum state, which allows detecting of eavesdropping. However, like classical key exchange protocols, QKD is vulnerable to man-in-the-middle attacks when used without authentication, because no known principle of quantum mechanics can distinguish between trusted and non-trusted entities.

> The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state. The no-cloning theorem has profound implications in the field of quantum computing and quantum communication.

Box 2.1: No-cloning theorem

Various products using quantum cryptography based on QKD are currently being developed or already commercially available from a number of vendors; for example:

- QKD components;
- QKD management software;
- QKD modules;
- QKD platforms.

Despite the fact that QKD is an innovative topic and still a lot of work is done in research, several standardisation documents exist already, addressing different areas of QKD. Both the European Telecommunications Standards Institute (ETSI) and the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) have published several standards for QKD (network) security and interoperability requirements. Also, an international standard (ISO/IEC 23837) for QKD security requirements is being developed.

OpenQKD is a European initiative that aims to act as a facilitator and multiplicator for QKD solutions. The cooperation of European academia, industry and start-ups on the deployment of open testbed sites across Europe, accessible for external stakeholders to perform field trials, is expected to significantly increase the awareness and facilitate the involvement with QKD.

Main QKD limitations are:

- only provides point-to-point secret key establishment between two endpoints on an optical fibre link without optical relays (aka optical amplifiers) or between two endpoints in line-of-sight in free space;
- works only over limited geographical distances (the current theoretical QKD distance limit is several 100 kilometres over optical fibre links, but this distance is much lower in practical implementations); this has motivated development of QKD Networks (QKDNs);
- requires special-purpose equipment and communication facilities, e.g. specialised photon transmitters and receivers and typically also requires dedicated optical fibre links, which significantly increases ICT infrastructure costs;
- increases insider threat risks, e.g. because it necessitates the use of trusted relays to overcome distance limitations in QKDN networks;
- increases the risk of Denial-of-Service (DoS): attacks can be mounted by simply disrupting the dedicated communication link;
- fragmented QKD (network) standardisation;
- securing and validating QKD implementations is a significant challenge.

Current commercially available QKD solutions are predominantly aimed at governments and other (large) organisations with very high security requirements. Factors preventing wide adoption of QKD include the cost of equipment and the lack of a demonstrated classical threat to existing classical secret key exchange schemes. Nonetheless, these classical secret key exchange schemes are not believed to provide sufficient security guarantees in very high-security environments, hence key distribution by means of physical transport (e.g. using courier services) is typically used in such environments. Compared to QKD, there is no intrinsic distance limit and, of importance when the One-Time Pad (OTP) cryptographic scheme is used, despite long travel times, the key transfer rate can be high due to the availability of large-capacity portable storage devices. For such use cases, the major advantages of QKD, compared to physical key transport, are its ability to detect any interception of the key and its fully automatic nature.

2.3.3. QKD Network (QKDN)

Incumbent network service providers and a growing number of start-up companies are currently developing QKD-based network services, and many others are in the process of developing such services. China has implemented the world's largest QKD-based communication network, combining over 700 optical fibres on the ground with two ground-to-satellite links to achieve QKD over a total distance of 4,600 km across the country. Other examples of QKD networks:

- British Telecom London metropolitan QKDN;
- DARPA Quantum Network;
- DLR satellite QKDN;
- Haven van Rotterdam metropolitan QKDN;
- NATO Quantum VPN;
- New York Quantum Metro Network;
- QuTech/Juniper Networks/Eurofiber QKDN testbed;
- South Korea Telcom QKDN;
- Swissquantum QKDN;
- UK Quantum Network;
- US DoD drone-based QKDN.

2.3.4. Other quantum security mechanisms

There is ongoing research into how existing classical cryptographic techniques, other than secret key exchange, public-key encryption and digital signatures, have to be modified to be able to cope with quantum computing adversaries. New security mechanisms that are based on the unique properties of quantum mechanics are also being researched.

Current research on quantum cryptography beyond QRNG and QKD includes the following (in alphabetical order):

- Blind Quantum Computation (BQC);
- position-based quantum cryptography;
- Quantum Anonymous Broadcasting (QAB);
- quantum commitment;
- Quantum Conference Key Agreement (QCKA);
- Quantum Digital Signature (QDS);
- Quantum Entity Authentication (QEA) aka Quantum Secure Authentication (QSA);
- quantum fingerprinting;
- Quantum Hash Function (QHF);
- quantum homomorphic cryptography;
- Quantum Message Authentication Code (QMAC);
- quantum money;
- quantum one-way function;
- Quantum Permutation Pad (QPP);
- quantum Physical Unclonable Function (qPUF);
- quantum pseudotelepathy;
- quantum public-key encryption;
- Quantum Secret Sharing (QSS);
- Quantum Secure Aggregation (QSA);

- Quantum Secure Direct Communication;
- Quantum Secure Time Transfer (QSTT);
- quantum teleportation;
- quantum voting.

There are several theoretical proposals for most of these quantum cryptography topics but currently only a few experimental implementations are known.

Appendix A – References

[ACM 1996] Lov Kumar Grover - A fast quantum mechanical algorithm for database search (Proceedings of the 28th annual symposium on theory of computing)

[ANSSI et al. 2024] Position Paper on Quantum Key Distribution

[ETSI 2013] Michele Mosca - Setting the scene the ETSI quantum-safe cryptography workshop (E-proceedings of the 1st Quantum-Safe-Crypto Workshop)

[IEEE 1994] Peter Williston Shor - Algorithms for quantum computation: discrete logarithms and factoring (Proceedings of the 35th annual symposium on foundations of computer science)

Appendix B - Acronyms and abbreviations

ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
aka	also known as
ANSI	American National Standards Institute
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
API	Application Programming Interface
ASC	Accredited Standards Committee
AWS	Amazon Web Services
BIKE	Bit Flipping Key Encapsulation
bit	binary digit
BQC	Blind Quantum Computation
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDN	Content Delivery Network
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Electrotechnique
CIRCL	Cloudflare Interoperable, Reusable Cryptographic Library
CROSS	Codes and Restricted Objects Signature Scheme
CRQC	Cryptographically Relevant Quantum Computer
CRYSTALS	Cryptographic Suite for Algebraic Lattices
DARPA	Defense Advanced Research Projects Agency
DES	Data Encryption Standard
DH	Diffie-Hellman
DLP	Discrete Logarithm Problem
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DoD	Department of Defense
DoS	Denial-of-Service

e.g.	exempli gratia
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
EITCI	European Information Technologies Certification Institute
EQRNG	Entanglement-based Quantum Random Number Generator
et al.	et alia
etc.	et cetera
ETSI	European Telecommunications Standards Institute
FALCON	Fast-*F*ourier Lattice-based Compact *Si*gnatures *o*ver NTRU
FFT	Fast-Fourier Transform
FIDO2	Fast I*d*entity Online 2
FIPS	Federal Information Processing Standards
FN-DSA	FFT over NTRU-Lattice-Based Digital Signature Algorithm
FTQC	Fault-Tolerant Quantum Computer
GNFS	General Number Field Sieve
HAWK	a pun on “FALCON”
HQC	Hamming Quasi-Cyclic
HSM	Hardware Security Module
HSS	Hierarchical Signature System
IBM	International Business Machines
i.e.	id est
ICM	Index-Calculate Method
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IFP	Integer Factorisation Problem
IoT	Internet of Things
IP	Internet Protocol
IPsec	IP security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization *S*ector
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
km	kilometre
LESS	Linear Equivalence Signature Scheme
LMS	Leighton-Micali Scheme
MAYO	a pun on “Oil and Vinegar”
MD5	Message Digest 5
MIRA	MInRAnk
MiRithH	MinRank in the Head
ML-DSA	Module-Lattice-Based Key-Encapsulation Mechanism
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
MPC	Multi-Party Computation
MQ	Multivariate Quadratic
MQOM	MQ-*o*n-my-Mind
NATO	North Atlantic Treaty Organization
NBV	Nationaal Bureau voor Verbindingsbeveiliging
NCSC	Nationaal Cyber Security Centrum National Cyber Security Centre
NEQRNG	Non Entanglement-based Quantum Random Number Generator
NIST	National Institute of Standards and Technology
NOVA	Noncommutative Oil and Vinegar with Alignment
NSA	National Security Agency
NTRU	N-th *D*egree Truncated *P*olynomial Ring Units

OEM	Original Equipment Manufacturer
OQS	Open Quantum Safe
OTP	One-Time Pad
PC	Personal Computer
PCIe	Peripheral Component Interconnect *E*xpress
PERK	PERmuted Kernel
PQC	Post-Quantum Cryptography
PQCA	Post-Quantum Cryptography Alliance
PUF	Physically Unclonable Function
Q-EaaS	Quantum Entropy-as-a-Service
Q-PUF	Quantum Physically Unclonable Function
QAB	Quantum Anonymous Broadcasting
QCKA	Quantum Conference Key Agreement
QDS	Quantum Digital Signature
QEA	Quantum Entity Authentication
QFFT	Quantum Fast Fourier Transform
QHF	Quantum Hash Function
QHSM	Quantum Hardware Security Module
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QMAC	Quantum Message Authentication Code
QPP	Quantum Permutation Pad
qPUF	quantum Physical Unclonable Function
QR-UOV	Quotient Ring UOV
QRC	Quantum-Resistant Cryptography
QRNG	Quantum Random Number Generator
QSA	Quantum Secure Aggregation
	Quantum-Secure Authentication
QSG	Quantum Standards Group

QSS	Quantum Secret Sharing
QSTT	Quantum Secure Time Transfer
qubit	quantum bit
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SCA	Side-Channel Attack
SDiTH	Syndrome Decoding-in-the-Head
SHA-2	Secure Hash Algorithm 2
SIKE	Supersingular Isogeny Key Encapsulation
SNOVA	Simple NOVA
SPHINCS+	Stateless Practical Hash-based Incredibly Nice Cryptographic Signatures plus
SQIsign	Short Quaternion and Isogeny signature
SSD	Solid-State Disk
SSH	Secure SHell
TLS	Transport Layer Security
TPM	Trusted Platform Module
UK	United Kingdom
UOV	Unbalanced Oil and Vinegar
US	United States
USB	Universal Serial Bus
VM	Virtual Machine
VMI	Virtual Machine Image
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
XMSS	eXtended Merkle Signature Scheme
XMSSMT	Multi-*t*ree XMSS